UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/918,062	07/30/2001	Keith Alexander Harrison	30006786-2	2570

7590 02/16/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 02/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/918,062	HARRISON ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 November 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 30 November 2005 has been entered.

2. By the above submission, Claims 1, 5, 9, 18, and 19 have been amended. No claims have been added or canceled. Claims 1-19 are currently pending in the present application.

Response to Arguments

3. Applicant's arguments with respect to claims 1-19 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

4. Claims 1 and 9 are objected to because of the following informalities:

Both Claims 1 and 9, in the last lines of each claim, recite "the second token that is uniquely related to the first token of the intended recipient". Although it is clear that this refers to the second token of the intended recipient and not to the second token of the sender, the Examiner recommends that the claim be amended to explicitly recite that this is the second token of the intended recipient.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claim 3 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 3 recites the limitation "the obtaining step"; however, it is not clear whether this is intended to refer to, in Claim 1, the step of "obtaining a second token" or the step of "obtaining a first token". This renders the claim indefinite.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-12 and 14-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Linsker et al, US Patent 5598473, in view of Mazzagatte et al, US Patent 6862583, and Menezes et al, *Handbook of Applied Cryptography*.

In reference to Claims 1, 5, and 8, Linsker discloses a method for determining the authenticity of a fax document (column 2, lines 23-27) that includes receiving a document and a digest of the document created by a hash algorithm and encrypted with a first token of the sender, which is the sender's private key (column 4, lines 54-60, where digest signature DS is the encrypted digest); obtaining a second token of the sender, which is the sender's public key, relating to the private key (column 4, lines 57-65); decrypting the digest with the public key (column 5, lines 20-23); creating a second digest using a hash algorithm (column 5, lines 23-27, and column 4, lines 25-35); and comparing the decrypted received digest with the second created digest (column 5, lines 23-42). However, although Linsker discloses authenticating the sender of a document, Linsker does not explicitly disclose verifying the identity of the intended recipient of a document.

Mazzagatte discloses a method for authenticated secure printing, which can be implemented for fax documents (column 4, lines 35-37), and which includes receiving and securely retaining a digital document and a transmitted independently verifiable data record of an intended recipient at a printout station (column 8, line 20-column 9, line 7; noting column 8, line 63-column 9, line1, where the data is securely stored at the

printer; further noting column 8, lines 20-29, where the digital certificate is the independently verifiable data record); obtaining a first token of the intended recipient, which is the recipient's private key (column 4, lines 9-12); requesting proof of the intended recipient's identity at the printout station using the independently verifiable data record (column 9, lines 49-51); and releasing the document when the intended recipient's identity has been proven by use of a second token of the intended recipient that is related to the recipient's first token, where the second token is the recipient's public key (column 9, lines 46-62). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Linsker by including verification of the intended recipient in addition to authentication of the sender, in order to ensure that printout of sensitive documents is authorized and that print data is securely stored (see Mazzagatte, column 2, lines 7-10).

Although Mazzagatte and Linsker disclose that the independently verifiable data record includes identification data (Mazzagatte, column 8, lines 20-30) and that a challenge/response protocol is used to authenticate and prove the intended recipient's identity (Mazzagatte, column 9, lines 58-61), Mazzagatte and Linsker do not explicitly disclose that the challenge/response protocol decrypts encrypted identification data with the recipient's private key, where the identification data was encrypted with the recipient's public key. However, Menezes discloses that challenge-response identification and authentication can be performed based on public-key decryption (page 403, Section 10.3.3, first paragraph). Menezes further discloses that the protocol includes encrypting a challenge, which can be an identifier, with a public key, decrypting

the encrypted challenge with a private key to form the response, comparing the challenge and response, and verifying the identity if the comparison result indicates a match (page 404, "(i) Challenge-response based on public-key decryption"). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Linsker and Mazzagatte by implementing the challenge/response protocol in the manner suggested by Menezes, in order to identify the recipient based on its private key (page 403, Section 10.3.3, first paragraph) and avoid chosen text attacks (page 404, paragraph "Identification based on PK decryption and witness").

In reference to Claims 2 and 3, Linsker, Mazzagatte, and Menezes further disclose receiving a digital certificate of the sender and that the public key is part of the certificate (see Linsker, column 5, lines 2-13).

In reference to Claim 4, Linsker, Mazzagatte, and Menezes further disclose checking the validity of the certificate online (see Linsker, column 5, lines 6-13).

In reference to Claims 6 and 7, Linsker, Mazzagatte, and Menezes further disclose printing the document with a verifying mark once it has been authenticated (see Linsker, column 6, lines 3-29).

In reference to Claims 9, 10, and 17, Linsker discloses a method of sending a fax document (column 2, lines 23-27) that includes creating a digest of the document using a hash algorithm (column 4, lines 25-35); encrypting the digest with a first token of the sender, which is the sender's private key (column 4, lines 40-47); obtaining a second

token of the sender, specifically the sender's public key, that will be used to decrypt the encrypted digest; and sending the encrypted digest, the document, and the public key to the recipient (column 4, lines 50-53). However, although Linsker discloses authenticating the sender of a document, Linsker does not explicitly disclose verifying the identity of the intended recipient of a document.

Mazzagatte discloses a method for authenticated secure printing, which can be implemented for fax documents (column 4, lines 35-37), and which includes receiving and securely retaining a digital document and a transmitted independently verifiable data record of an intended recipient at a printout station (column 8, line 20-column 9, line 7; noting column 8, line 63-column 9, line1, where the data is securely stored at the printer; further noting column 8, lines 20-29, where the digital certificate is the independently verifiable data record); obtaining a first token of the intended recipient, which is the recipient's private key (column 4, lines 9-12); requesting proof of the intended recipient's identity at the printout station using the independently verifiable data record (column 9, lines 49-51); and releasing the document when the intended recipient's identity has been proven by use of a second token of the intended recipient that is related to the recipient's first token, where the second token is the recipient's public key (column 9, lines 46-62). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Linsker by including verification of the intended recipient in addition to authentication of the sender, in order to ensure that printout of sensitive documents is authorized and that print data is securely stored (see Mazzagatte, column 2, lines 7-10).

Although Mazzagatte and Linsker disclose that the independently verifiable data record includes identification data (Mazzagatte, column 8, lines 20-30) and that a challenge/response protocol is used to authenticate and prove the intended recipient's identity (Mazzagatte, column 9, lines 58-61), Mazzagatte and Linsker do not explicitly disclose encrypting identification information of the recipient with the recipient's public key, nor do Mazzagatte and Linsker explicitly disclose that the challenge/response protocol decrypts the encrypted identification data with the recipient's private key. However, Menezes discloses that challenge-response identification and authentication can be performed based on public-key decryption (page 403, Section 10.3.3, first paragraph). Menezes further discloses that the protocol includes encrypting a challenge, which can be an identifier, with a public key, decrypting the encrypted challenge with a private key to form the response, comparing the challenge and response, and verifying the identity if the comparison result indicates a match (page 404, "(i) Challenge-response based on public-key decryption"). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Linsker and Mazzagatte by implementing the challenge/response protocol in the manner suggested by Menezes, in order to identify the recipient based on its private key (page 403, Section 10.3.3, first paragraph) and avoid chosen text attacks (page 404, paragraph "Identification based on PK decryption and witness").

In reference to Claims 11 and 12, Linsker, Mazzagatte, and Menezes further disclose proving the sender's identity by transferring data from a personal portable data carrier holding the private key to the transmission station from which the document will

be sent, and that the sender enters a verifiable security identifier to establish the sender's identity (see Linsker, column 7, lines 13-21).

In reference to Claims 14-16, Linsker, Mazzagatte, and Menezes further disclose obtaining details of the sender, including the public key, from a central database, and providing the details and public key in a digital certificate (see Linsker, column 4, lines 50-53; column 5, lines 2-13).

Claims 18 and 19 are apparatus claims corresponding substantially to the methods of Claims 1 and 9, and are rejected by a similar rationale.

9. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Linsker in view of Mazzagatte and Menezes as applied to claim 11 above, and further in view of Clark, US Patent 5448045.

Linsker, Mazzagatte, and Menezes disclose everything as applied above in reference to Claim 11. However, Linsker, Mazzagatte, and Menezes do not explicitly disclose that the digest is encrypted within the personal portable data carrier. Clark discloses that digital signatures (formed by encrypting a message digest with a private key) can be performed in smart cards (column 8, lines 53-58). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Linsker, Mazzagatte, and Menezes to include encrypting the digest within the personal portable data carrier, in order to prevent compromise of the sender's private key (see Clark, column 8, lines 57-62).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER